Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the instant application:

Listing of Claims:

1. (Currently Amended) A method for managing a presentation of sensitive content in non-trusted environments, comprising the steps of:

interrogating a list of policies associated with a given user and a physical device;

determining a location of the physical device;

comparing the location of the physical device with a list of trusted locations;

providing access to a subscription-based service that maintains an organization list of individuals and machine identification information indicating that a listed individual or machine is associated with a predetermined organization;

determining that an individual or machine identified on the list is within a predetermined proximity of the physical device, and in response thereto, transmitting an alert to the physical device;

and

enforcing a plurality of rules contained in the policy for managing the presentation of sensitive content[[,]] ~~wherein access to sensitive information is limited or restricted based on the location~~ by blocking a visual presentation or audible presentation of at least one object in portions of the presentation if the physical device is not located in a trusted location or if an individual or a machine identified on the organization list is within a predetermined proximity of the physical device.

2. (Previously Presented) The method of claim 1, wherein the method further comprises the step of providing a reminder of the policy regarding confidential material

to the given user in response to an attempt to access sensitive information on the physical device.

3. (Previously Presented) The method of claim 1, wherein the method further comprises the step of requesting authentication from the given user in response to an attempt to access sensitive information in an open application on the physical device.

4. (Original) The method of claim 3, wherein the step of requesting authentication comprises at least one among requesting provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user.

5. (Original) The method of claim 1, wherein the step of determining a location comprises the step of using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device.

6. (Currently Amended) The method claim 1, wherein the step of enforcing comprises at least one among blacking out a visual object in a display during the presentation, replacing a visual object with innocuous content during the presentation, visually hiding the [[the]] at least one object from the given user during the presentation, and inserting audio 'white noise' gaps in an audio object.

7. (Currently Amended) A system for managing a presentation of sensitive content in non-trusted environments, comprising:

a memory;

a display; and

a processor coupled to the memory and the display, wherein the processor is programmed to:

interrogate a list of policies associated with a given user and a physical device;

determine a location of the physical device;

compare the location of the physical device with a list of trusted locations;

access a subscription-based service that maintains an organization list of individuals and machine identification information indicating that a listed individual or machine is associated with a predetermined organization;

determine that an individual or machine identified on the list is within a predetermined proximity of the physical device, and in response thereto, transmitting an alert to the physical device; and

enforce a plurality of rules contained in the policy for managing the presentation of sensitive content[[,]] ~~wherein access to sensitive information is limited or restricted based on the location~~ by blocking a visual presentation or audible presentation of at least one object in portions of the presentation if the physical device is not located in a trusted location or if an individual or a machine identified on the organization list is within a predetermined proximity of the physical device.

8. (Previously Presented) The system of claim 7, wherein the processor is further programmed to provide a reminder of the policy regarding confidential material to the given user in response to an attempt to access sensitive information on the physical device.

9. (Previously Presented) The system of claim 7, wherein the processor is further programmed to request authentication from the given user in response to an attempt to access sensitive information in an open application on the physical device.

10. (Original) The system of claim 9, wherein the processor requests authentication by requesting at least one among the provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user.

11. (Original) The system of claim 7, wherein the processor determines the location by using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device.

12. (Currently Amended) The system of claim 7, wherein the processor enforces the policies by at least one among blacking out a visual object in a display during the presentation, replacing a visual object with innocuous content during the presentation, visually hiding the [[the]] at least one object from the given user during the presentation and inserting audio 'white noise' gaps in an audio object.

13. (Currently Amended) A machine-readable storage, having stored thereon a computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

interrogating a list of policies associated with a given user and a physical device;

determining a location of the physical device;

comparing the location of the physical device with a list of trusted locations;

providing access to a subscription-based service that maintains an organization list of individuals and machine identification information indicating that a listed individual or machine is associated with a predetermined organization;

determining that an individual or machine identified on the list is within a predetermined proximity of the physical device, and in response thereto, transmitting an alert to the physical device; and

enforcing a plurality of rules contained in the policy for managing the presentation of sensitive content[[,]] ~~wherein access to sensitive information is limited or restricted based on the location~~ by blocking a visual presentation or audible presentation of at least one object in portions of the presentation if the physical device is not located in a trusted location or if an individual or a machine identified on the organization list is within a predetermined proximity of the physical device.

14. (Previously Presented) The machine-readable storage of claim 13, wherein the computer program further comprises a plurality of code sections for causing the machine to provide a reminder of the policy regarding confidential material to the given user in response to an attempt to access sensitive information on the physical device.

15. (Previously Presented) The machine-readable storage of claim 13, wherein the computer program further comprises a plurality of code sections for causing to request authentication from the given user in response to an attempt to access sensitive information in an open application on the physical device.

16. (Original) The machine-readable storage of claim 15, wherein the computer program requests authentication by requesting at least one among a provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user.

17. (Original) The machine-readable storage of claim 13, wherein the computer program determines a location by using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device.

18. (Currently Amended) The machine-readable storage claim 13, wherein the computer program enforces the policy by at least one among blacking out a visual object in a display during the presentation, replacing a visual object with innocuous content during the presentation, visually hiding the [[the]] at least one object from the given user during the presentation and inserting audio 'white noise' gaps in an audio object.

19. (Cancelled)

20. (Previously Presented) The method of claim 3, further comprising
identifying a seniority level of the given user; and
granting a permission to override the policy based on the seniority.